What is claimed is:

1. A key agreement system comprising a shared-key generation apparatus and a shared-key recovery apparatus, each apparatus establishing therein a same shared key in secrecy, wherein

the shared-key generation apparatus includes:

a seed-value generating unit operable to generate a seed value;

a first shared-key generating unit operable to generate a blind value and a shared key, from the seed value;

an encryption unit operable to encrypt the seed value based on the blind value, to generate encryption information; and

a transmitting unit operable to transmit the encryption information, and

the shared-key recovery apparatus includes:

a receiving unit operable to receive the encryption information;

a decryption unit operable to decrypt the encryption information, to generate a decryption seed value;

a second shared-key generating unit operable to generate a decryption blind value and a decryption shared

key, using the decryption seed value and according to a same method as used in the first shared-key generating unit;

a re-encryption unit operable to encrypt the decryption seed value based on the decryption blind value, to generate re-encryption information;

a judging unit operable to judge, based on the encryption information and the re-encryption information, whether the decryption shared key should be outputted; and

an outputting unit operable, when the judging unit has judged affirmatively, to output the decryption shared key.

2. The key agreement system of Claim 1, wherein

the shared-key generation apparatus further includes:

an obtaining unit operable to obtain a content; and

an encryption unit operable to encrypt the obtained content using the shared key, to generate an encrypted content,

the transmitting unit further transmits the encrypted content,

the receiving unit further receives the encrypted content, and

the shared-key recovery apparatus further includes:

a decryption unit operable to decrypt the received encrypted content using the decryption shared key, to generate a decrypted content; and

an outputting unit operable to output the decrypted content.

3. A shared-key generation apparatus that notifies a destination apparatus about a shared key in secrecy, the shared-key generation apparatus comprising:

a seed-value generating unit operable to generate a seed value;

a shared-key generating unit operable to generate a blind value and a shared key, from the seed value;

an encryption unit operable to encrypt the seed value based on the blind value, to generate encryption information; and

a transmitting unit operable to transmit the encryption information.

4. The shared-key generation apparatus of Claim 3, wherein

the shared-key generating unit performs a one-way function on the seed value, to generate a functional value,

and generates the blind value and the shared key from the functional value,

the encryption unit includes:

a public-key obtaining subunit operable to obtain a public key; and

a public-key encryption subunit operable to perform a public-key encryption algorithm on the seed value, using the public key and the blind value, to generate an encryption seed value as the encryption information.

5. The shared-key generation apparatus of Claim 4, wherein

the public-key encryption algorithm conforms to an NTRU cryptosystem,

the public-key obtaining subunit obtains a public-key polynomial generated according to a key-generation algorithm of the NTRU cryptosystem, as the public key,

the public-key encryption subunit generates a seed-value polynomial from the seed value, generates a blind-value polynomial from the blind value, and encrypts the seed-value polynomial according to an encryption algorithm of the NTRU cryptosystem, using the public-key polynomial as a key, and using the blind-value polynomial to randomize the seed-value polynomial, to generate an

encryption seed-value polynomial as the encryption seed value, and

the transmitting unit transmits the encryption seed-value polynomial as the encryption seed value.

6. The shared-key generation apparatus of Claim 3, wherein

the encryption unit includes:

a public-key obtaining subunit operable to obtain a public key;

a public-key encryption subunit operable to generate a blind value, perform the public-key encryption algorithm on the seed value using the public key and the blind value, to generate a public-key cipher text; and

a function subunit operable to perform a second one-way function on at least one of the seed value, the blind value, and the shared key, to generate a second functional value, and

the encryption unit generates the encryption information that includes the public-key cipher text and the second functional value.

7. The shared-key generation apparatus of Claim 6, wherein

the shared-key generating unit performs a one-way function on the seed value, to generate a functional value, and generates the blind value and the shared key from the functional value.

8. The shared-key generation apparatus of Claim 6, wherein

the shared-key generating unit performs a first one-way function on the seed value, to generate a first functional value, and generates the shared key from the first functional value, instead of generating the blind value and the shared key.

9. The shared-key generation apparatus of Claim 6, wherein

the public-key encryption algorithm conforms to an NTRU cryptosystem,

the public-key obtaining subunit obtains a public-key polynomial generated according to a key-generation algorithm of the NTRU cryptosystem, as the public key,

the public-key encryption subunit generates a seed-value polynomial from the seed value, generates a blind-value polynomial from the blind value, encrypts the seed-value polynomial according to an encryption algorithm

of the NTRU cryptosystem, using the public-key polynomial as a key, and using the blind-value polynomial to randomize the seed-value polynomial, to generate an encryption seed-value polynomial as the public-key cipher text, and

the encryption unit generates the encryption information that includes the encryption seed-value polynomial as the public-key cipher text and the second functional value.

10. The shared-key generation apparatus of Claim 3, wherein

the shared-key generating unit performs a one-way function on the seed value, to generate a functional value, and generates a verification value, the blind value, and the shared key, from the functional value,

the encryption unit includes:

a public-key obtaining subunit operable to obtain a public key;

a first encryption subunit operable to perform a public-key encryption algorithm on the verification value, using the public key and the blind value, to generate a first cipher text; and

a second encryption subunit operable to perform, on the seed value, a computation algorithm different from

the public-key encryption algorithm, to generate a second cipher text, and

the encryption unit generates the encryption information that includes the first cipher text and the second cipher text.

11. The shared-key generation apparatus of Claim 10, wherein

the public-key encryption algorithm conforms to an NTRU cryptosystem,

the public-key obtaining subunit obtains a public-key polynomial generated according to a key-generation algorithm of the NTRU cryptosystem, as the public key,

the first encryption subunit generates a verification-value polynomial from the verification value, generates a blind-value polynomial from the blind value, and encrypts the verification-value polynomial according to an encryption algorithm of the NTRU cryptosystem, using the public-key polynomial as a key, and using the blind-value polynomial to randomize the verification-value polynomial, to generate an encryption verification-value polynomial as the first cipher text, and

the encryption unit generates the encryption information that includes the encryption

verification-value polynomial as the first cipher text and the second cipher text.

12. The shared-key generation apparatus of Claim 11, wherein

the different computation algorithm is a symmetric key encryption algorithm, and

the second encryption subunit performs the symmetric key encryption algorithm on the seed value using the verification value as a key, to generate the second cipher text.

13. The shared-key generation apparatus of Claim 11, wherein

the different computation algorithm is bitwise exclusive-or, and

the second encryption subunit performs the bitwise exclusive-or on the verification value and the seed value, to generate the second cipher text.

14. The shared-key generation apparatus of Claim 11, wherein

the different computation algorithm is addition, and

the second encryption subunit performs the addition

on the verification value and the seed value, to generate the second cipher text.

15. The shared-key generation apparatus of Claim 11, wherein

the different computation algorithm is multiplication, and

the second encryption subunit performs the multiplication on the verification value and the seed value, to generate the second cipher text.

16. The shared-key generation apparatus of Claim 3, wherein

the seed-value generating unit generates a random number, as the seed value.

17. The shared-key generation apparatus of Claim 3, wherein

the shared-key generating unit performs a one-way function on the seed value, to generate a functional value, and generates the blind value and the shared key from the functional value.

18. The shared-key generation apparatus of Claim 17,

wherein

the one-way function is a hash function, and

the shared-key generating unit performs the hash function on the seed value.

19. The shared-key generation apparatus of Claim 17, wherein

the shared-key generating unit generates the blind value by setting a part of the functional value as the blind value, and generates the shared key by setting another part of the functional value as the shared key.

20. The shared-key generation apparatus of Claim 3, further comprising:

an obtaining unit operable to obtain a content; and

an encryption unit operable to encrypt the obtained content using the shared key, to generate an encrypted content, wherein

the transmitting unit further transmits the encrypted content.

21. A shared-key recovery apparatus that receives a shared key from a shared-key generation apparatus in secrecy, the shared-key generation apparatus generating a seed value,

generating a blind value and a shared key from the seed value, encrypting the seed value based on the blind value to generate encryption information, and transmitting the encryption information, the shared-key recovery apparatus comprising:

a receiving unit operable to receive the encryption information;

a decryption unit operable to decrypt the encryption information, to generate a decryption seed value;

a shared-key generating unit operable to generate a decryption blind value and a decryption shared key, using the decryption seed value and according to a same shared-key generating method used in the shared-key generation apparatus;

a re-encryption unit operable to encrypt the decryption seed value based on the decryption blind value, to generate re-encryption information;

a judging unit operable to judge, based on the encryption information and the re-encryption information, whether the decryption shared key should be outputted; and

an outputting unit operable, when the judging unit has judged affirmatively, to output the decryption shared key.

22. The shared-key recovery apparatus of Claim 21, wherein

the shared-key generation apparatus performs a one-way function on the seed value to generate a functional value, generates the blind value and the shared key from the functional value, obtains a public key, performs a public-key encryption algorithm on the seed value using the public key and the blind value, to generate an encryption seed value as the encryption information, and transmits the encryption seed value,

the receiving unit receives the encryption seed value as the encryption information,

the decryption unit includes:

a secret-key obtaining subunit operable to obtain a secret key that corresponds to the public key; and

a public-key decryption subunit operable to perform, on the received encryption seed value, a public-key decryption algorithm that corresponds to the public-key encryption algorithm, using the obtained secret key, to generate the decryption seed value,

the shared-key generating unit performs the one-way function on the decryption seed value to generate a decryption functional value, and generates the decryption blind value and the decryption shared key from the decryption functional value,

the re-encryption unit includes:

a public-key obtaining subunit operable to obtain the public key; and

a re-encryption subunit operable to perform the public-key encryption algorithm on the decryption seed value using the public key and the decryption blind value, to generate a re-encryption seed value as the re-encryption information, and

the judging unit judges whether the encryption seed value is identical to the re-encryption seed value, and when judging affirmatively, determines that the decryption shared key should be outputted.

23. The shared-key recovery apparatus of Claim 22, wherein

the public-key encryption algorithm and the public-key decryption algorithm conform to an NTRU cryptosystem,

the shared-key generation apparatus obtains a public-key polynomial generated according to a key-generation algorithm of the NTRU cryptosystem, as the public key, generates a seed-value polynomial from the seed value, generates a blind-value polynomial from the blind value, encrypts the seed-value polynomial according to an encryption algorithm of the NTRU cryptosystem, using the

public-key polynomial as a key, and using the blind-value polynomial to randomize the seed-value polynomial, to generate an encryption seed-value polynomial as the encryption seed value, and transmits the encryption seed-value polynomial as the encryption seed value,

the receiving unit receives the encryption seed-value polynomial as the encryption seed value,

the secret-key obtaining subunit obtains a secret-key polynomial generated according to the key-generation algorithm of the NTRU cryptosystem, as the secret key,

the public-key decryption subunit decrypts the received encryption seed-value polynomial according to a decryption algorithm of the NTRU cryptosystem and using the obtained secret-key polynomial as a key, to generate a decryption seed-value polynomial, and generates the decryption seed value from the decryption seed-value polynomial,

the public-key obtaining subunit obtains the public-key polynomial as the public key,

the re-encryption subunit generates a seed-value polynomial from the decryption seed value, generates a blind-value polynomial from the decryption blind value, and encrypts the seed-value polynomial according to the encryption algorithm of the NTRU cryptosystem, using the

public-key polynomial as a key, and using the blind-value polynomial to randomize the seed-value polynomial, to generate a re-encryption seed-value polynomial, and

the judging unit judges whether the encryption seed-value polynomial is identical to the re-encryption seed-value polynomial.

24. The shared-key recovery apparatus of Claim 21, wherein

the shared-key generation apparatus obtains a public key, generates a blind value, performs a public-key encryption algorithm on the seed value using the public key and the blind value to generate a public-key cipher text, performs a second one-way function on at least one of the seed value, the blind value, and the shared key to generate a second functional value, generates the encryption information that includes the public-key cipher text and the second functional value, and transmits the encryption information,

the receiving unit receives the encryption information that includes the public-key cipher text and the second functional value,

the decryption unit includes:

a secret-key obtaining subunit operable to obtain a secret key that corresponds to the public key;

a public-key decryption subunit operable to perform, on the public-key cipher text included in the received encryption information, a public-key decryption algorithm that corresponds to the public-key encryption algorithm, to generate a decryption seed value; and

a function subunit operable to perform the second one-way function on at least one of the decryption seed value, the decryption blind value, and the decryption shared key, to generate a decryption second functional value, and

the judging unit judges whether the second functional value included in the received encryption information is identical to the decryption second functional value instead of performing judging based on the encryption information and the re-encryption information, and when judging affirmatively, determines that the decryption shared key should be outputted.

25. The shared-key recovery apparatus of Claim 24, wherein

the shared-key generation apparatus performs a one-way function on the seed value to generate a functional value, and generates the blind value and the shared key from the functional value, and

the shared-key generating unit performs the first one-way function on the decryption seed value to generate

a decryption functional value, and generates the decryption blind value and the decryption shared key from the decryption functional value.

26. The shared-key recovery apparatus of Claim 24, wherein

the shared-key generation apparatus performs a first one-way function on the seed value to generate a first functional value, and generates the shared key from the first functional value, instead of generating the blind value and the shared key, and

the shared-key generating unit performs the first one-way function on the decryption seed value to generate a decryption functional value, and generates the decryption shared key from the decryption functional value, instead of generating the decryption blind value and the decryption shared key.

27. The shared-key recovery apparatus of Claim 24, wherein

the public-key encryption algorithm and the public-key decryption algorithm conform to an NTRU cryptosystem,

the shared-key generation apparatus obtains a public-key polynomial generated according to a key-generation algorithm of the NTRU cryptosystem, as the

public key, generates a seed-value polynomial from the seed value, generates a blind-value polynomial from the blind value, encrypts the seed-value polynomial according to an encryption algorithm of the NTRU cryptosystem using the public-key polynomial as a key and using the blind-value polynomial to randomize the seed-value polynomial, to generate an encryption seed-value polynomial as the public-key cipher text, and generates the encryption information that includes the encryption seed-value polynomial as the public-key cipher text and the second functional value,

the secret-key obtaining subunit obtains a secret-key polynomial generated according to the key-generation algorithm of the NTRU cryptosystem, as the secret key, and

the public-key decryption subunit generates a public-key cipher-text polynomial from the public-key cipher text, decrypts the public-key cipher-text polynomial according to a decryption algorithm of the NTRU cryptosystem using the secret-key polynomial as a key to generate a decryption seed-value polynomial, and generates the decryption seed value from the decryption seed-value polynomial.

28. The shared-key recovery apparatus of Claim 21, wherein

the shared-key generation apparatus performs a one-way function on the seed value to generate a functional value, generates a verification value, the blind value, and the shared key from the functional value, obtains a public key, performs a public-key encryption algorithm on the verification value using the public key and the blind value to generate a first cipher text, performs, based on the verification value, a computation algorithm different from the public-key encryption algorithm on the seed value, to generate a second cipher text, generates the encryption information that includes the first cipher text and the second cipher text, and transmits the encryption information,

the receiving unit receives the encryption information that includes the first cipher text and the second cipher text,

the decryption unit includes:

a secret-key obtaining subunit operable to obtain a secret key that corresponds to the public key;

a public-key decryption subunit operable to perform, on the first cipher text included in the received encryption information, a public-key decryption algorithm that corresponds to the public-key encryption algorithm, to generate a decryption verification value; and

a computation decryption subunit operable to perform, on the second cipher text included in the received encryption information, a computation algorithm for performing an inverse computation of the different computation algorithm, to generate a decryption seed value,

the shared-key generating unit performs the one-way function on the decryption seed value to generate a decryption functional value, and generates a decryption verification value, the decryption blind value, and the decryption shared key, from the decryption functional value,

the re-encryption unit includes:

a public-key obtaining subunit operable to obtain the public key; and

a re-encryption subunit operable to perform, on the decryption verification value, the public-key encryption algorithm using the public key and the decryption blind value, to generate the re-encryption information, and

the judging unit judges whether the first cipher text included in the encryption information is identical to the re-encryption information, and when judging affirmatively, determines that the decryption shared key should be outputted.

29. The shared-key recovery apparatus of Claim 28, wherein

the public-key encryption algorithm and the public-key decryption algorithm conform to an NTRU cryptosystem,

the shared-key generation apparatus obtains a public-key polynomial generated according to a key-generation algorithm of the NTRU cryptosystem, as the public key, generates a verification-value polynomial from the verification value, generates a blind-value polynomial from the blind value, encrypts the verification-value polynomial according to an encryption algorithm of the NTRU cryptosystem, using the public-key polynomial as a key, and using the blind-value polynomial to randomize the verification-value polynomial, to generate an encryption verification-value polynomial as the first cipher text, generates the encryption information that includes the encryption verification-value polynomial as the first cipher text and the second cipher text, and transmits the encryption information,

the receiving unit receives the encryption information that includes the encryption verification-value polynomial and the second cipher text,

the secret-key obtaining subunit obtains a secret-key polynomial generated according to the key-generation

algorithm of the NTRU cryptosystem, as the secret key,

the public-key decryption subunit generates a first cipher-text polynomial from the first cipher text, decrypts the first cipher-text polynomial according to a decryption algorithm of the NTRU cryptosystem using the secret-key polynomial as a key, to generate a decryption verification polynomial, and generates the decryption verification value from the decryption verification-value polynomial,

the public-key obtaining subunit obtains the public-key polynomial,

the re-encryption subunit generates a decryption verification-value polynomial from the decryption verification value, generates a blind-value polynomial from the decryption blind value, and encrypts the decryption verification-value polynomial according to the encryption algorithm of the NTRU cryptosystem, using the public-key polynomial as a key, and using the blind-value polynomial to randomize the decryption verification-value polynomial, to generate a re-encryption verification-value polynomial as the re-encryption information, and

the judging unit judges whether the encryption verification-value polynomial as the first cipher text is identical to the re-encryption verification-value polynomial as the re-encryption information.

30. The shared-key recovery apparatus of Claim 29, wherein the different computation algorithm is a symmetric key encryption algorithm, and the computation algorithm for performing the inverse computation is a corresponding symmetric key decryption algorithm, and

the computation decryption subunit performs the symmetric key decryption algorithm on the second cipher text, using the decryption verification value as a key, to generate the decryption seed value.

31. The shared-key recovery apparatus of Claim 29, wherein the different computation algorithm and the computation algorithm for performing the inverse computation are bitwise exclusive-or, and

the computation decryption subunit performs the bitwise exclusive-or on the decryption verification value and the second cipher text, to generate the decryption seed value.

32. The shared-key recovery apparatus of Claim 29, wherein the different computation algorithm is addition and the computation algorithm for performing the inverse computation is subtraction, and

the computation decryption subunit performs the

subtraction on the decryption verification value and the second cipher text, to generate the decryption seed value.

33. The shared-key recovery apparatus of Claim 29, wherein the different calculation algorithm is multiplication and the computation algorithm for performing the inverse computation is division, and

the computation decryption subunit performs the division on the decryption verification value and the second cipher text, to generate the decryption seed value.

34. The shared-key recovery apparatus of Claim 21, wherein the shared-key generating unit performs a one-way function on the decryption seed value to generate a functional value, and generates the decryption blind value and the decryption shared key from the functional value.

35. The shared-key recovery apparatus of Claim 34, wherein the one-way function is a hash function, and the shared-key generating unit performs the hash function on the decryption seed value.

36. The shared-key recovery apparatus of Claim 34, wherein the shared-key generating unit generates the

decryption blind value by setting a part of the functional value as the decryption blind value, and generates the decryption shared key by setting another part of the functional value as the decryption shared key.

37. The shared-key recovery apparatus of Claim 21, wherein the shared-key generation apparatus further obtains a content, encrypts the obtained content using the shared key to generate an encrypted content, and transmits the encrypted content, and

the shared-key recovery apparatus further includes:

a content receiving unit operable to receive the encrypted content;

a decryption unit operable to decrypt the received encrypted content using the outputted decryption shared key, to generate a decrypted content; and

a playback unit operable to playback the decrypted content.

38. A shared-key generating method used in a shared-key generation apparatus that notifies a destination apparatus about a shared key in secrecy, the shared-key generating method comprising:

a seed-value generating step of generating a seed

value;

a shared-key generating step of generating a blind value and a shared key, from the seed value;

an encryption step of encrypting the seed value based on the blind value, to generate encryption information; and

a transmitting step of transmitting the encryption information.

39. A shared-key generating program used in a shared-key generation apparatus that notifies a destination apparatus about a shared key in secrecy, the shared-key generating program comprising:

a seed-value generating step of generating a seed value;

a shared-key generating step of generating a blind value and a shared key, from the seed value;

an encryption step of encrypting the seed value based on the blind value, to generate encryption information; and

a transmitting step of transmitting the encryption information.

40. The shared-key generating program of Claim 39, wherein

the shared-key generating program is recorded in a computer-readable recording medium.

41. A shared-key recovery method used in a shared-key recovery apparatus that receives a shared key from a shared-key generation apparatus in secrecy, the shared-key generation apparatus generating a seed value, generating a blind value and a shared key from the seed value, encrypting the seed value based on the blind value to generate encryption information, and transmitting the encryption information, the shared-key recovery method comprising:

a receiving step of receiving the encryption information;

a decryption step of decrypting the encryption information, to generate a decryption seed value;

a shared-key generating step of generating a decryption blind value and a decryption shared key, using the decryption seed value and according to a same shared-key generating method used in the shared-key generation apparatus;

a re-encryption step of encrypting the decryption seed value based on the decryption blind value, to generate re-encryption information;

a judging step of judging, based on the encryption

information and the re-encryption information, whether the decryption shared key should be outputted; and

an outputting step, when the judging unit has judged affirmatively, of outputting the decryption shared key.

42. A shared-key recovery program used in a shared-key recovery apparatus that receives a shared key from a shared-key generation apparatus in secrecy, the shared-key generation apparatus generating a seed value, generating a blind value and a shared key from the seed value, encrypting the seed value based on the blind value to generate encryption information, and transmitting the encryption information, the shared-key recovery program comprising:

a receiving step of receiving the encryption information;

a decryption step of decrypting the encryption information, to generate a decryption seed value;

a shared-key generating step of generating a decryption blind value and a decryption shared key, using the decryption seed value and according to a same shared-key generating method used in the shared-key generation apparatus;

a re-encryption step of encrypting the decryption seed value based on the decryption blind value, to generate

re-encryption information;

a judging step of judging, based on the encryption information and the re-encryption information, whether the decryption shared key should be outputted; and

an outputting step, when the judging unit has judged affirmatively, of outputting the decryption shared key.

43. The shared-key recovery program of Claim 42, wherein

The shared-key recovery program is recorded in a computer-readable recording medium.